Searching PAJ

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-013614
(43)Date of publication of application : 14.01.2000

(51)Int.Cl. H04N 1/44
G06F 17/30
G06F 19/00
H04L 9/36
H04N 1/21
H04N 1/387

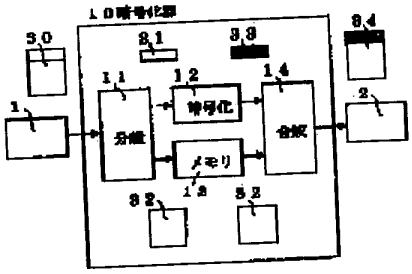
(21)Application number : 10-178484
(22)Date of filing : 25.06.1998

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>
(72)Inventor : SAKANO TOSHIKAZU
YAMAGUCHI TAKAHIRO
FURUSAKI KAZUNORI

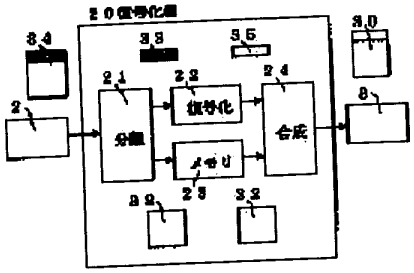
(54) IMAGE DATA COMMUNICATION SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a medical image data communication system which is fast and also has high safety with a simple configuration in a medical image data communication system that has enciphering and decoding means.
SOLUTION: This medical image data communication system which has a transmitting means which transmits medical image data 30 consisting of an image data body 32 and accompanying information accompanying the body 32, a communication network which transmits the data 30 transmitted by the transmitting means and a receiving means which receives the data transmitted through the communication network. In such a case, the data 30 are divided into the body 32 and the accompanying information by utilizing the fact that the data 30 do not make sense until both the body 32 and text data representing the accompanying information are put together and only the accompany information is enciphered by an enciphering device that has high safety. Thus, it is possible to reduce processing time that is needed for enciphering and decoding without damaging safety in medial image data communication drastically and to economically realize medical image data communication that has high safety.

(a)



(b)



LEGAL STATUS
[Date of request for examination] 22.12.2000
[Date of sending the examiner's decision of rejection] 24.09.2002
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]

Searching PAJ

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2000－13614
（P2000－13614A）
(43)公開日　平成12年１月14日(2000.1.14)

(51)Int.Cl.'	識別記号	FI		テーマコード'（参考）
H04N 1/44		H04N 1/44		5B075
G06F 17/30			1/21	5C073
19/00			1/387	5C075
H04L 9/36		C06F 15/40	370B	5C076
H04N 1/21			15/42 X	5K013

審査請求　未請求　請求項の数４　ＯＬ　（全 10 頁）　最終頁に続く

(21)出願番号　特願平10－178484
(22)出願日　平成10年６月25日(1998.6.25)

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(72)発明者　坂野　寿和
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内
(72)発明者　山口　高弘
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内
(74)代理人　100083552
弁理士　秋田　収喜

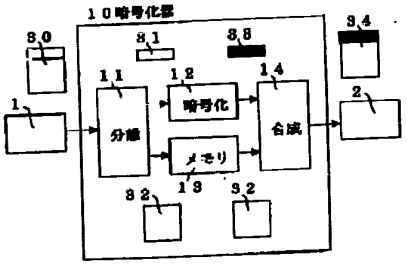
最終頁に続く

(54)【発明の名称】　画像データ通信システム

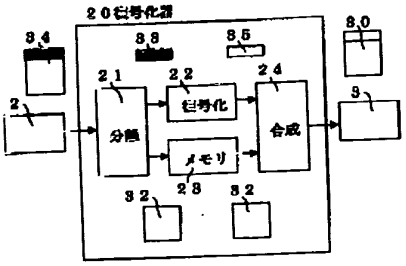
(57)【要約】
【課題】　暗号化、復号化手段を有する医療画像データ通信システムにおいて、簡便な構成で高速、かつ、安全性の高い医療画像データ通信システムを提供する。
【解決手段】　画像データ本体と前記画像データ本体に付随する付随情報からなる医療画像データを送信する送信手段と、前記送信手段により送出された前記医療画像データを伝送する通信網と、前記通信網を介して伝送された前記医療画像データを受信する受信手段とを有する医療画像データ通信システムにおいて、医療画像データが画像データ本体と付随情報を表すテキストデータの両者が揃ってはじめて意味のあるデータになるという性質を利用し、医療画像データを画像データ本体と付随情報とに分離し、付随情報のみを安全性の高い暗号化装置で暗号化する。これにより、医療画像データ通信における安全性を損なうことなく暗号化、復号化にかかる処理時間を大幅に短縮することができ、安全性の高い医療画像データ通信を経済的に実現することを可能とする。

図１

（ａ）



（ｂ）



【特許請求の範囲】

【請求項1】 画像データ本体と前記画像データ本体に付随する付随情報からなる画像データを送信する送信手段と、前記送信手段により送出された前記画像データを伝送する通信網と、前記通信網を介して伝送された前記画像データを受信する受信手段とを有する画像データ通信システムにおいて、前記送信手段は、前記画像データを画像データ本体と付随情報とに分離する分離手段と、前記分離手段により分離した前記付随情報を暗号化する暗号化手段と、前記暗号化手段により付随情報を暗号化している間、画像データ本体を一時格納しておくメモリと、前記暗号化手段により暗号化された前記付随情報と前記メモリに一時格納されていた前記画像データ本体とを合成する合成手段を有し、前記受信手段は、伝送された前記画像データを画像データと暗号化された付随情報とに分離する分離手段と、前記分離手段により分離した前記付随情報を復号化する復号化手段と、前記復号化手段により付随情報を復号化している間、画像データ本体を一時格納しておくためのメモリと、前記復号化手段により復号化された前記付随情報と前記メモリに一時格納されていた前記画像データ本体とを合成する合成手段とを有することを特徴とする画像データ通信システム。

【請求項2】 画像データ本体と前記画像データ本体に付随する付随情報からなる画像データを送信する送信手段と、前記送信手段により送出された前記画像データを伝送する通信網と、前記通信網を介して伝送された前記画像データを受信する受信手段とを有する画像データ通信システムにおいて、前記送信手段は、前記画像データを画像データ本体と付随情報とに分離する分離手段と、前記分離手段により分離した前記付随情報を暗号化する第1の暗号化手段と、前記分離手段により分離した前記画像データ本体を暗号化する第2の暗号化手段と、前記第1の暗号化手段により暗号化された前記付随情報と前記第2の暗号化手段により暗号化された前記画像データ本体とを合成する合成手段を有し、前記受信手段は、伝送された前記画像データを暗号化された画像データ本体と暗号化された付随情報とに分離する分離手段と、前記分離手段により分離した前記付随情報を復号化する第1の復号化手段と、前記分離手段により分離した前記画像データ本体を復号化する第2の復号化手段と、前記第1の復号化手段により復号化された前記付随情報と前記第2の復号化手段により復号化された前記画像データ本体とを合成する手段を有する画像データ通信システムであって、前記画像データ本体に対する第2の暗号化、復号化手段が、前記付随情報に対する第1の暗号化、復号化手段に比べて単位データ当りの信号処理量が少ない暗号化、復号化手段であることを特徴とする画像データ通信システム。

【請求項3】 画像データ本体と前記画像データ本体に付随する付随情報からなる画像データを送信する送信手段と、前記送信手段により送出された前記画像データを伝送する通信網と、前記通信網を介して伝送された前記画像データを受信する受信手段とを有する画像データ通信システムにおいて、前記送信手段は、前記画像データ本体に付随情報の一部が記載されている場合に前記付随情報の一部を消去する消去手段と、前記画像データを画像データ本体と付随情報とに分離する分離手段と、前記分離手段により分離した付随情報を暗号化する暗号化手段と、前記暗号化手段により付随情報を暗号化している間、前記画像データ本体を一時格納しておくためのメモリと、前記暗号化手段により暗号化された前記付随情報と前記メモリに一時格納しておいた画像データ本体とを合成する合成手段を有し、前記受信手段は、伝送された前記画像データを画像データ本体と暗号化された付随情報とに分離する分離手段と、前記分離手段により分離した前記付随情報を復号化する復号化手段と、前記復号化手段により付随情報を復号化している間、一時格納しておくためのメモリと、前記復号化手段により復号化された前記付随情報と前記メモリに一時格納しておいた前記画像データ本体とを合成する合成手段とを有することを特徴とする画像データ通信システム。

【請求項4】 画像データ本体と前記画像データ本体に付随する付随情報からなる画像データを送信する送信手段と、前記送信手段により送出された前記画像データを伝送する通信網と、前記通信網を介して伝送された前記画像データを受信する受信手段とを有する画像データ通信システムにおいて、前記送信手段は、前記画像データ本体に付随情報の一部が記載されている場合に前記付随情報の一部を消去する消去手段と、前記画像データを画像データ本体と付随情報とに分離する分離手段と、前記分離手段により分離した付随情報を暗号化する第1の暗号化手段と、前記分離手段により分離した前記画像データ本体を暗号化する第2の暗号化手段と、前記第1の暗号化手段により暗号化された前記付随情報と前記第2の暗号化手段により暗号化された前記画像データ本体とを合成する合成手段を有し、前記受信手段は、伝送された前記画像データを暗号化された画像データ本体と暗号化された付随情報とに分離する分離手段と、前記分離手段により分離した前記付随情報を復号化する第1の復号化手段、前記分離手段により分離した前記画像データ本体を復号化する第2の復号化手段と、前記第1の復号化手段により復号化された前記付随情報と前記第2の復号化手段により復号化された前記画像データ本体とを合成する合成手段を有する画像データ通信システムであって、前記画像データ本体に対する第2の暗号化、復号化手段が、前記付随情報に対する第1の暗号化、復号化手段に比べて単位データ当りの信号処理量が少ない暗号化、復号化手段であることを特徴とする画像データ通信システム。

【発明の詳細な説明】

【0001】
【発明が属する技術分野】本発明は、ディジタル画像データの通信システムに関し、特に、医療画像データの通信に適用して有効な技術に関するものである。
【0002】
【従来の技術】医療現場で用いられる医療画像は、X線画像、CT画像、MRI画像、病理画像、内視鏡画像、超音波画像など多岐にわたっている。
【0003】これら医療画像の伝送、蓄積、保存は、個々の画像の取得形態に応じて異なる形で行われてきた。例えば、X線画像はX線フィルム上に記録され、このフィルムをシャーカステンと呼ばれるビューワー上に置いて画像を観察することから、X線フィルム自体を送付、蓄積、保存することが長年にわたって行われてきた。
【0004】また、病理画像は人体の組織や細胞を染色し顕微鏡で拡大表示したもので、そのサンプル本体であるプレパラートや顕微鏡画像を撮影した写真を送付、蓄積、保存していた。その他の医療画像についても、フィルムや写真などを使ったほぼ同様の伝送、蓄積、保存方法が取られていた。
【0005】しかし、近年のコンピュータ及びその周辺技術の向上にともない、これらの医療画像をスキャナなどを用いてデジタルデータ化する医療画像の電子化が急速な勢いで普及しつつある。デジタルデータ化された医療画像（以下、医療画像データという）は電子メモリ媒体（半導体メモリ、磁気メモリ、光磁気メモリなど）に蓄積、保存され、必要に応じてコンピュータディスプレイ上に表示される。
【0006】また、通信網を介してこれらの医療画像データを病院内外へ転送することもデジタル通信網が整備されるにつれて容易かつ経済的に実現できるようになってきた。このように医療画像の電子化とデジタルネットワーク化の進展により、医療画像データの転送が場所や時間に関係なく瞬時に行うことが可能となり、遠隔医療や在宅医療などこれらの技術を用いた種々の医療サービス形態も現実のものとなりつつある。デジタル通信網を使ったこのような新しい医療形態の出現により医師、患者の利便性を格段に向上させることができる。
【0007】図4は従来の医療画像データ通信システムの概略構成を示すブロック構成図である。通信網2を介して接続されるのは、病院間、患者宅と病院間、検査機関と病院間、個人院と大病院間など様々なケースが考えられる。図4では、医療画像データ表示装置3と医療画像データが蓄積されている医療画像データベース1とが通信網2を介して接続されている場合である。
【0008】まず、医療画像データ表示装置3を持つ医療画像データ受信者5から前記医療画像データベース1に対して医療画像データ転送要求が送信される。医療画像データベース1を持つ医療画像データ送信者4は、医療画像データの転送要求に基づいて医療画像データベース1から所望の医療画像データを検索し、通信網2に検索した医療画像データを送出する。医療画像データ受信者5は、通信網2から医療画像データを受信してそれを医療画像データ表示装置3によって表示する。
【0009】通信網2を介して授受される医療画像データは、放射線画像などの画像データ本体とそれに付随した付随情報、すなわち、検査年月日、検査医療施設、患者ID、患者名、生年月日、性別、検査装置、診断情報、検査部位、検査技師名、診断医師名などである。このような付随情報を含んだ医療画像データのデータフォーマットについては、ACR-NEMA（the American College of Radiology and the National Electrical Manufactures Association）などの団体によって標準化が進められている。
【0010】一般に、医療画像データは高解像度、多階調であることが要求される。例えば、胸部放射線画像のディジタル画像データには画素数2000×2000以上、階調が10～12ビット以上が必要であると言われている。そのため医療画像データはデータ量が大きく、画像1枚あたり数MB（メガバイト）となることも多い。
【0011】医療画像データには患者のプライバシーに関わる情報が含まれているので、他人にデータを盗み見されることがないよう、通信ネットワークには高い信頼性が要求される。病院内LANなどでネットワークが閉じていれば、病院内での管理を徹底することによりある程度の信頼性を確保することはできる。一方、病院間で医療画像データ通信を実施する場合にはデータ漏洩が起きないように専用線を用いるなど他人が介入できないネットワークを利用するのが普通である。
【0012】しかしながら、将来の医療画像データ通信では、様々なネットワークを介して医療画像データの通信が行われることが想定される。病院内はもとより、病院間での医療画像データの転送による遠隔診断（支援）や、患者宅から病院へ、あるいは個人院から大病院への医療画像データの転送などが考えられる。このような様々な階層で必要に応じて医療画像データの通信を実施する場合に、それぞれに対して専用線を設けて通信することは現実的ではない。
【0013】そこで、一般的な通信網を介して医療画像データの授受が行われることが想定される。場合によっては、インターネットなどのコネクションレス型ネットワーク中を医療画像データが往来する状況も考えられる。一般の通信網を用いて医療画像データを安全に転送するためには暗号化技術の適用など画像通信の安全性を高めるための施策が必要不可欠である。
【0014】これは、図4に示す通り、医療画像データベース1と通信網2、通信網2と医療画像表示装置3の間にそれぞれ暗号化器6、復号化器7を設け、医療画像データを通信網2に送出する際には医療画像データを暗

号化して送出する。

【0015】また、通信網2を介して送られてきた暗号化された医療画像データは、受信側で復号化器7によって元のデータに変換されて医療画像表示装置3に入力される。このように通信網内では暗号化された医療画像データが往来するようにすることで、一般の通信網を用いても医療画像データ通信の信頼性を確保することが可能となる。医療画像データの暗号化、復号化装置としては、秘密鍵暗号装置、公開鍵暗号装置など種々の装置が提案されており、これらを適用することができる。

【0016】

【発明が解決しようとする課題】しかしながら、従来の暗号化技術を備えた医療画像データ通信装置では、安全性を高めるために困難性の大きな暗号化装置を適用しようとすると、医療画像データのデータ量が大きいために処理時間の増大が顕著になるという問題があった。

【0017】図5（a）及び（b）は、従来の医療画像データの暗号化装置の性質を定性的に説明するための図であり、（a）は医療画像データの一般的なフォーマットを示し、（b）は暗号化、復号化データ量と暗号化、復号化にかかる処理時間の関係を定性的に示している。図5（a）に示すように、医療画像データ30は医療画像データ本体31とそれに付随する付随情報（患者ID、患者名、生年月日、性別、検査年月日、検査装置、診断情報、部位、検査実施者、診断医師名など）32が一体化されている。通常、画像データ本体31のデータ量は数MB（メガバイト）、付随情報32はテキストデータなので数KB（キロバイト）であり、全体として数MB（メガバイト）以上の大きな容量となる。図5（b）は暗号化、復号化データ量と暗号化、復号化にかかる処理時間の関係を定性的に示しており、暗号化方式Aの方が、暗号化方式Bと比較して解読困難度が高く、安全性が高い暗号化方式であることを示している。

【0018】一般に、暗号化、復号化するデータ量が多くなると、それに比例して暗号化、復号化にかかる処理時間は長くなる。また、高い安全性を持つ暗号化装置ほど暗号化、復号化にかかる処理時間は長くなる。ここで、安全性とは第3者が暗号を解読しようとする際の困難度である。安全性が高い程処理時間が大きくなるのは、大抵の暗号化技術が、素因数分解の困難性、離散対数問題の困難性などの数学的問題に基づいており、暗号化するけた数を大きくするほど解読困難性が増大し、それにつれて暗号化、復号化処理時間も増大するためである。

【0019】この問題を軽減するために処理時間の少ない暗号化方法を適用すると、通信時の安全性が低下するという問題が生じる。また、処理速度の大きなプロセッサなどを適用することにより暗号化、復号化にかかる処理時間の短縮を図ろうとすると、暗号化、復号化にかかる処理装置が高価になるという問題があった。

【0020】本発明の目的は、暗号化、復号化手段を有する画像データ通信システムにおいて、簡便な構成で高速、かつ、安全性の高い画像データ通信システムを提供することにある。本発明の前記ならびにその他の目的及び新規な特徴は、本明細書の記述及び添付図面によって明らかになるであろう。

【0021】

【課題を解決するための手段】本願において開示される発明のうち代表的なものの概要を簡単に説明すれば、下記の通りである。

（1）画像データ本体と前記画像データ本体に付随する付随情報からなる画像データを送信する送信手段と、前記送信手段により送出された前記画像データを伝送する通信網と、前記通信網を介して伝送された前記画像データを受信する受信手段とを有する画像データ通信システムにおいて、前記送信手段は、前記画像データを画像データ本体と付随情報とに分離する分離手段と、前記分離手段により分離した前記付随情報を暗号化する暗号化手段と、前記暗号化手段により付随情報を暗号化している間、画像データ本体を一時格納しておくメモリと、前記暗号化手段により暗号化された前記付随情報と前記メモリに一時格納されていた前記画像データ本体とを合成する合成手段を有し、前記受信手段は、伝送された前記画像データを画像データと暗号化された付随情報とに分離する分離手段と、前記分離手段により分離した前記付随情報を復号化する復号化手段と、前記復号化手段により付随情報を復号化している間、画像データ本体を一時格納しておくためのメモリと、前記復号化手段により復号化された前記付随情報と前記メモリに一時格納されていた前記画像データ本体とを合成する合成手段とを有する。

【0022】（2）画像データ本体と前記画像データ本体に付随する付随情報からなる画像データを送信する送信手段と、前記送信手段により送出された前記画像データを伝送する通信網と、前記通信網を介して伝送された前記画像データを受信する受信手段とを有する画像データ通信システムにおいて、前記送信手段は、前記画像データを画像データ本体と付随情報とに分離する分離手段と、前記分離手段により分離した前記付随情報を暗号化する第1の暗号化手段と、前記分離手段により分離した前記画像データ本体を暗号化する第2の暗号化手段と、前記第1の暗号化手段により暗号化された前記付随情報と前記第2の暗号化手段により暗号化された前記画像データ本体とを合成する合成手段を有し、前記受信手段は、伝送された前記画像データを暗号化された画像データ本体と暗号化された付随情報とに分離する分離手段と、前記分離手段により分離した前記付随情報を復号化する第1の復号化手段と、前記分離手段により分離した前記画像データ本体を復号化する第2の復号化手段と、前記第1の復号化手段により復号化された前記付随情報

と前記第2の復号化手段により復号化された前記画像データ本体とを合成する手段を有する画像データ通信システムであって、前記画像データ本体に対する第2の暗号化、復号化手段が、前記付随情報に対する第1の暗号化、復号化手段に比べて単位データ当りの信号処理量が少ない暗号化、復号化手段である。

【0023】(3)画像データ本体と前記画像データ本体に付随する付随情報からなる画像データを送信する送信手段と、前記送信手段により送出された前記画像データを伝送する通信網と、前記通信網を介して伝送された前記画像データを受信する受信手段とを有する画像データ通信システムにおいて、前記送信手段は、前記画像データ本体に付随情報の一部が記載されている場合に前記付随情報の一部を消去する消去手段と、前記画像データを画像データ本体と付随情報とに分離する分離手段と、前記分離手段により分離した付随情報を暗号化する暗号化手段と、前記暗号化手段により付随情報を暗号化している間、前記画像データ本体を一時格納しておくためのメモリと、前記暗号化手段により暗号化された前記付随情報と前記メモリに一時格納しておいた画像データ本体とを合成する合成手段を有し、前記受信手段は、伝送された前記画像データを画像データ本体と暗号化された付随情報とに分離する分離手段と、前記分離手段により分離した前記付随情報を復号化する復号化手段と、前記復号化手段により付随情報を復号化している間、一時格納しておくためのメモリと、前記復号化手段により復号化された前記付随情報と前記メモリに一時格納しておいた前記画像データ本体とを合成する合成手段とを有する。

【0024】(4)画像データ本体と前記画像データ本体に付随する付随情報からなる画像データを送信する送信手段と、前記送信手段により送出された前記画像データを伝送する通信網と、前記通信網を介して伝送された前記画像データを受信する受信手段とを有する画像データ通信システムにおいて、前記送信手段は、前記画像データ本体に付随情報の一部が記載されている場合に前記付随情報の一部を消去する消去手段と、前記画像データを画像データ本体と付随情報とに分離する分離手段と、前記分離手段により分離した付随情報を暗号化する第1の暗号化手段と、前記分離手段により分離した前記画像データ本体を暗号化する第2の暗号化手段と、前記第1の暗号化手段により暗号化された前記付随情報と前記第2の暗号化手段により暗号化された前記画像データ本体とを合成する合成手段を有し、前記受信手段は、伝送された前記画像データを暗号化された画像データ本体と暗号化された付随情報とに分離する分離手段と、前記分離手段により分離した前記付随情報を復号化する第1の復号化手段、前記分離手段により分離した前記画像データ本体を復号化する第2の復号化手段と、前記第1の復号化手段により復号化された前記付随情報と前記第2の復号化手段により復号化された前記画像データ本体とを合成する合成手段を有する画像データ通信システムであって、前記画像データ本体に対する第2の暗号化、復号化手段が、前記付随情報に対する第1の暗号化、復号化手段に比べて単位データ当りの信号処理量が少ない暗号化、復号化手段である。

【0025】すなわち、本発明は、画像データが画像データ本体と付随情報を表すテキストデータの両者が揃ってはじめて意味のあるデータになるという性質を利用し、画像データを画像データ本体と付随情報とに分離し、付随情報のみを安全性の高い暗号化装置で暗号化することを最も主要な特徴とする画像データ通信システムである。

【0026】前記の手段によれば、画像データ通信に於ける安全性を損なうことなく暗号化、復号化にかかる処理時間を大幅に短縮することができ、安全性の高い画像データ通信を経済的に実現することができる。

【0027】以下、本発明について、図面を参照して実施形態(実施例)とともに詳細に説明する。

【0028】

【発明の実施の形態】(実施形態1)本発明の実施形態1及び2は、本発明の画像通信システムを医療画像通信システムに適用したものである。

【0029】図1は本発明の実施形態(実施例)1の医療画像通信システムの概略構成を示すためのブロック構成図であり、図1(a)は本実施例の暗号化器構成の概略構成を示すブロック構成図、図1(b)は本実施例の復号化器の概略構成を示すブロック構成図である。図1において、1は医療画像データベース、2は通信網、3は医療画像データ表示装置、10は暗号化器、11は入力された医療画像データを画像データ本体と付随情報とに分離するための分離手段、12は付随情報を暗号化するための暗号化手段、13は暗号化処理中に画像データ本体を一時格納しておくためのメモリ、14は暗号化された付随情報と画像データ本体を合成するための合成手段、16は画像データ本体を暗号化するための暗号化手段、17は暗号化された付随情報と暗号化された画像データ本体を合成するための合成手段、20は復号化器、21は入力された医療画像データを暗号化された付随情報と画像データ本体に分離するための分離手段、22は暗号化された付随情報を復号化するための復号化手段、23は復号化処理中、画像データ本体を一時格納しておくためのメモリ、24は復号化された付随情報と画像データ本体を合成するための合成手段、26は入力された医療画像データを暗号化された付随情報と暗号化された画像データ本体に分離するための分離手段、27は暗号化された画像データ本体を復号化するための復号化手段、28は復号化された付随情報と復号化された画像データ本体とを合成するための合成手段、30はDICOMフォーマットの医療画像データ、31は付随情報、32は画像データ本体、33は暗号化された付随情報、3

４は付随情報のみが暗号化された医療画像データ、３５は復号化された付随情報である。

【００３０】まず、暗号化器１０に入力された医療画像データ３０は、分離手段１１により画像データ本体３２とそれに付随する付随情報を表すテキストデータ（以下、付随情報という）３１とに分離される。分離した付随情報３１は暗号化手段１２によって暗号化され、暗号化された付随情報３３になる。付随情報３１の暗号化処理中、画像データ本体３２はメモリ１３に格納されている。暗号化処理が終わると、暗号化された付随情報３３とメモリ１３に格納されていた画像データ本体３２とは合成手段１４によって合成され、医療画像データ３４として送出される。前記暗号化器１０から送出される医療画像データ３４は付随情報部のみに安全性の高い暗号化装置で暗号化がなされていることになる。

【００３１】一方、復号化器２０に入力された医療画像データ３４は、分離手段２１により画像データ本体３２と暗号化された付随情報３３に分離される。分離した暗号化された付随情報３３は、復号化手段２２によって復号化され、復号化された付随情報３５になる。暗号化された付随情報３３の復号化処理中、画像データ本体３２はメモリ２３に格納されている。復号化処理が終わると、復号化された付随情報３５とメモリ２３に格納されていた画像データ本体３２とは合成手段２４によって合成され、医療画像データ３０に戻り出力される。

【００３２】データベースから伝送された医療画像データは、復号化器２０によって再合成された医療画像データ３０のように、画像データ本体３２と復号化された付随情報３５が揃って初めて意味のあるデータとなる。画像データ本体３２だけがあって、患者に関する情報や、医療画像に対する担当医師の診断結果、検査年月日などの付随情報がなければ、教科書に掲載されている医療画像あるいは学術的な雑誌に掲載されている医療画像と同じことであり、一般に広く公開されたとしても患者に対するプライバシーは完全に保護されることになる。

【００３３】本実施形態１では、画像データ本体３２は特に暗号化せず、付随情報３５のみを安全性の高い暗号化方法で暗号化する。付随情報３５のデータ量は画像データ本体３２のデータ量に比べて３桁近く少ないので、安全性の高い暗号化方法を用いても、画像データ全体を暗号化する場合に比べて暗号化、復号化にかかる信号処理量、ひいては処理時間を大幅に（３桁近く）減らすことができる。

【００３４】医療画像データ３０のフォーマットはＤＩＣＯＭに代表されるような標準化が進んでおり、医療画像データ３０を扱う各種機器（検査装置、データベース、表示装置、フィルムスキャナなど）は標準化された画像フォーマットに準拠している場合が多い。

【００３５】このため、本実施形態１の復号化器２０の出力において、画像データ本体３２と復号化された付随情報３５とを合成して医療画像データ３０として出力する構成を採ることにより、復号化器２０から出力された医療画像データ３０を、さらに他の医療画像データ関連装置へ転送し、表示させることも容易に実現することができる。

【００３６】（実施形態２）図２は本発明の実施形態（実施例）２の医療画像通信システムの概略構成を示すためのブロック構成図であり、図２（ａ）は本実施形態２の暗号化器構成の概略構成を示すブロック構成図、図２（ｂ）は本実施形態２の復号化器の概略構成を示すブロック構成図である。図２において、３は３６は暗号化された画像データ本体、３７は暗号化された付随情報３４と暗号化された画像データ本体３６からなる医療画像データ、３８は復号化された画像データ本体である。その他の符号は前記図１の実施形態１と同一機能を有するものである。

【００３７】本発明の実施形態（実施例）２の医療画像通信システムにおいて、暗号化器１５に入力された医療画像データ３０は、図２に示すように、分離手段１１により画像データ本体３２とそれに付随する付随情報３１とに分離される。分離した付随情報３１は、暗号化手段１２によって暗号化され、暗号化した付随情報３３になる。一方、分離した画像データ本体３２は、別の暗号化手段１６によって暗号化され、暗号化した画像データ本体３６になる。暗号化された付随情報３３と暗号化された画像データ本体３６は、合成手段１７によって合成され、医療画像データ３７として送出される。暗号化器１５から送出される医療画像データ３７は付随情報部分、画像データ本体部分の両方が暗号化されている。

【００３８】一方、復号化器２５に入力された医療画像データ３７は、分離手段２６により暗号化された画像データ本体３６と暗号化された付随情報３３とに分離される。分離した暗号化された付随情報３３は、復号化手段２２によって復号化され、復号化した付随情報３３になる。一方、暗号化された画像データ本体３６は、別の復号化手段２７によって復号化され、復号化された画像データ本体３８になる。復号化された付随情報３５と復号化された画像データ本体３８は、合成手段２８によって合成され、医療画像データ３０に戻り出力される。

【００３９】ここで、付随情報に対する暗号化、復号化は単位データ量あたりのデータ処理量が大きくなっても高い安全性を有する装置を用いる。一方、画像データ本体に対する暗号化、復号化は付随情報の場合と比較して単位データ量あたりのデータ処理量が少なくなるような装置を用いる。

【００４０】前記付随情報に対する暗号化手段１２として、例えば、けた数１５０～２００の素因数の合成数を用いた公開鍵暗号装置を用い、画像データ本体３６に対する暗号化手段１６として、例えば、けた数６４～１２８の素因数の合成数を用いた公開鍵暗号装置を用いるな

ど同じ暗号装置であっても画像データ本体に対する暗号化の桁数を少なくすることによって単位データ量当たりの処理量を小さくしても良い。

【００４１】また、画像データ本体３６に対する暗号化手段１６として、ある規則に従ったデータのランダム化を行ったり、あらかじめ通信する両者のみが持っているルックアップテーブルによってデータを変換するなど安全性は付随情報に対する暗号化手段１２より低く処理時間も短いが、素人は容易に解読出来ないような暗号化手段を採用してもよい。

【００４２】図３は本実施形態２における処理時間の特徴を説明するためのグラフである。

【００４３】横軸は暗号化、復号化データ量、縦軸は暗号化、復号化にかかる処理時間を表している。

【００４４】本実施形態２では、付随情報には安全性が高く単位データ当たりの処理量が大きい暗号化、復号化手段を採用し、画像データ本体には単位データ当たりの処理量が小さい暗号化、復号化手段を採用する。

【００４５】付随情報３１と画像データ本体３２のデータ量には3桁近い差があり、両者に対して処理時間の異なる暗号化手段を採用することにより全体の暗号化、復号化処理時間を小さく抑えることが可能となる。画像データ本体３２に対する暗号化手段の安全性が低くても、画像データ本体３２と付随情報３１の両方がそろって初めて価値のある医療画像データ３０となることを考えると、本実施形態２によって全体として医療画像データ通信システムの安全性を非常に高いものにすることができる。

【００４６】尚、前記実施形態１及び２では、画像データ本体３２には患者に関する情報などの付随情報は含まないことを前提としている。しかしながら、現状の医療分野においてフィルムベースの画像、あるいはフィルムをデジタライズした画像データ本体３２には、患者名、生年月日、年齢、医師名などが記載されている場合もある。このような場合、前記実施形態１及び２の医療画像データ通信システムでは、画像データ本体３２の安全性が低いため、画像データ本体３２に記載された付随情報を他人に盗み見られる可能性が高くなり、本発明の効果の一つである高い安全性の確保が実現できなくなる。

【００４７】そこで、画像データ本体３２に付随情報の一部が記載された医療画像データに対しては、医療画像データが本発明の暗号化器１０に入力される前に画像データ本体３２の付随情報が記載された部分を消去しておく必要がある。

【００４８】一般に、画像データ本体に付随情報が含まれる場合、画像の角付近（右上、右下、左下、左上の角など）に医療施設毎に決められたタグがついており、このタグに付随情報の一部が記載されているのが普通である。つまり、医療施設ごとにある程度決まったフォーマットで画像データ本体３２に付随情報が記載されていることから、画像をデジタルデータ化する際にその付随情報を自動的に消去することは容易にできる。

【００４９】例えば、ある病院で放射線フィルムの左上角に病院名、患者名、生年月日、年齢などを記載するフォーマットを適用しているとすると、フィルムデジタライザなどで電子データ化する際に、左上角の付随情報が記載された領域の画素値を自動的にゼロ（画面上で左上角は黒でつぶされる）にするよう、フィルムデジタライザをあらかじめ設定しておけば良い。

【００５０】また、これまでのフィルム等による画像管理では、このような画像本体に患者の名前などの付随情報が記載されている場合が多いが、検査装置からデジタル画像を直接取り込むような場合（放射線画像をダイレクトデジタライザにより取得した場合など）には画像データ本体に付随情報が記載されていることはないので、前記実施形態１及び２の医療画像データ通信システムをそのまま適用できる。

【００５１】例えば、医療画像データベースに記録されている医療画像データを読み出すことを、これまで説明してきた、つまり医療画像データベースから医療画像表示装置へ通信網を介して送る場合、データベース側で暗号化して表示装置側で復号化している。医療画像データの取り扱いはこの他に、表示装置側から新たな医療画像データを医療画像データベースへ送り記録することがある。この場合には表示装置側で暗号化してデータベース側で復号化する。従って、表示装置とデータベースは双方に通信が行われ、それぞれの側での暗号化器、復合化器を設置される。

【００５２】なお、前記実施形態では医療画像データ通信システムを本発明を適用した例で説明したが、本発明は一般の画像データ通信システムに通用できることは容易に推測できる。

【００５３】以上、本発明を実施形態（実施例）に基づき具体的に説明したが、本発明は、前記実施形態（実施例）に限定されるものではなく、その要旨を逸脱しない範囲において種々変更し得ることはいうまでもない。

【００５４】

【発明の効果】本願において開示される発明のうち、代表的なものによって得られる効果を簡単に説明すれば、下記の通りである。医療画像データが画像データ本体とそれに付随する付随情報によって構成され、両者がそろって初めて意味のあるデータになること、画像データ本体のデータ量は付随情報のデータ量に比べて３桁近く多いことなどの医療画像データ特有の性質を考慮し、付随情報には安全性の高い暗号化手法を適用し、画像データ本体には暗号化を施さないか、あるいは処理量の少ない暗号化方法を採用することにより、簡便な方法で高速かつ安全性の高い医療画像データ通信を実現できる。さらに、復号化器から出力された医療画像データのフォーマットが、元の医療画像データのフォーマットと同じなの

で、他の医療画像データ関連装置との医療画像データの授受を容易にできる。

【図面の簡単な説明】

【図１】本発明の実施形態（実施例）１の医療画像通信システムの概略構成を示すためのブロック構成図である。

【図２】本発明の実施形態（実施例）２の医療画像通信システムの概略構成を示すためのブロック構成図である。

【図３】本実施例２における医療画像データの暗号化、復号化の処理時間の特徴を説明するための図である。

【図４】従来の医療画像データ通信システムの概略構成を示すブロック構成図である。

【図５】従来の医療画像データの暗号化処理の性質を説明するための図である。

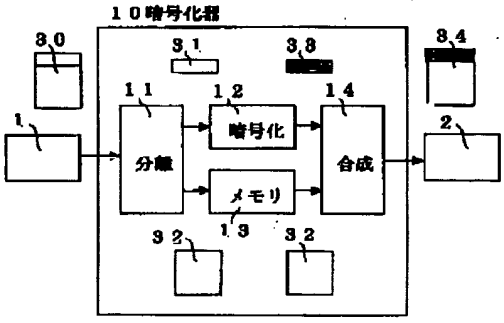
【符号の説明】

１…医療画像データベース、２…通信網、３…医療画像データ表示装置、４…医療画像データ送信者、５…医療画像データ受信者、６…暗号化器、７…復号化器、１０、１５…暗号化器、１１…分離手段、１２…暗号化手段、１３…メモリ、１４…合成手段、１６…暗号化手段、１７…合成手段、２０、２５…復号化器、２１…分離手段、２２…復号化手段、２３…メモリ、２４…合成手段、２６…分離手段、２７…復号化手段、２８…合成手段、３０…医療画像データ、３１…付随情報、３２…画像データ本体、３３…付随情報、３４…付随情報のみが暗号化された医療画像データ、３５…復号化された付随情報、３６…暗号化された画像データ本体、３７…医療画像データ、３８…復号化された画像データ本体。

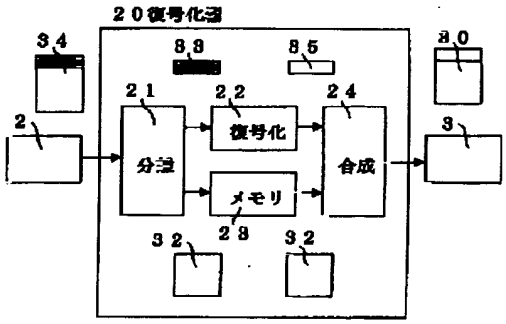
【図１】

図１

（ａ）



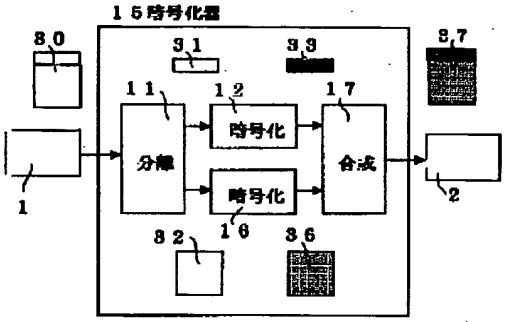
（ｂ）



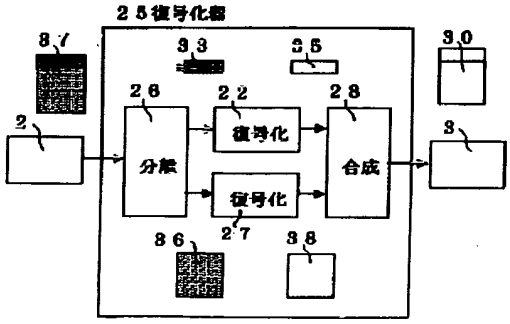
【図２】

図２

（ａ）

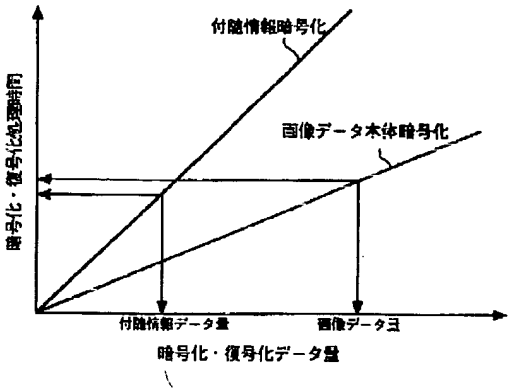


（ｂ）



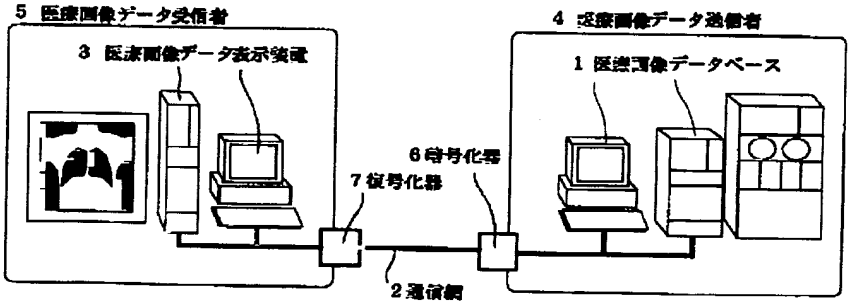
【図3】

図3



【図4】

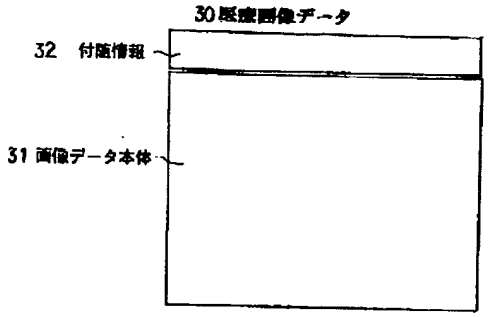
図4



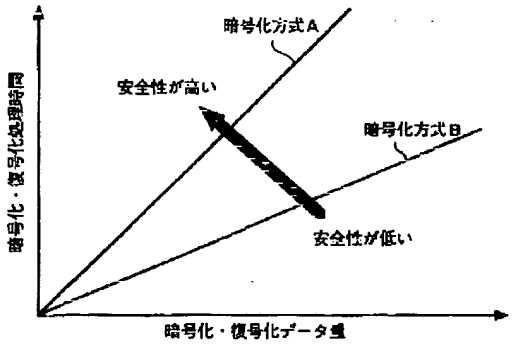
【図5】

図5

(a)



(b)



フロントページの続き

(51)Int.Cl.[7]	識別記号	FI		(参考)
H04N 1/387		H04L 9/00	685	

(72)発明者 古崎 和則
東京都新宿区西新宿三丁目19番2号 日本電信電話株式会社内

Fターム(参考) 5B075 KK22 KK33 ND07 ND08 UU29
5C073 AA02 AB11 BB01 BB07 CD12 CD22 CE09 CE10
5C075 CF05 CF90 EE03 FF90
5C076 AA14 AA40 BA06
5K013 BA00 BA05